Chapter 15
Security Deliverables

Chapter Overview

The annotated outlines in this chapter are all related to AIS security requirements for the United States Customs Service.

References

Much of the material in this chapter is based on information from:

- The Department of the Treasury *Security Manual*, TD P 71-10, 1992
- *Automated Information Systems Security Policy*, CIS HB 1400-05, 1996

Additional Information

If you require additional information or assistance with any of these deliverables, contact the AIS Security Division (AISSD).

In This Chapter

Continued on next page

Security Deliverables, Continued

In This Chapter (continued)

Section A
Deliverable Overviews

Section Overview

This section presents three types of overview data for the security deliverables.

- A brief description of each AIS Security document
- Table 15-1 showing when each deliverable is created, updated, baselined and revised (if necessary)
- Table 15-2 showing the prescribing directives for each security deliverable

Purpose

The overall purpose of these security deliverables is to:

- Ensure that appropriate security services are provided for each system
- Provide assurances that the security features work as claimed and cannot be easily defeated

Caveat

The tables provided show the security deliverable requirements as prescribed; the deliverable lists in the tables, however, include a number of items which are not defined as separate documents in this chapter. These information items may be covered elsewhere within the SDLC life cycle (e.g., Audits are included within Operation and Evaluation Phase activities) or as part of other documents.

The project must ensure that all required information is included within appropriate project documentation. To facilitate this, the Security Plan includes a section which can incorporate those items not included elsewhere.

Reference: Volume II, Chapter 1, Section C, *Tailoring Guidelines,* **Tailoring Security Deliverables**

Continued on next page

Deliverable Overviews, Continued

In This Section

Document Descriptions

Security Plan

The Security Plan documents all security-related activities. In the pre-operation phases of the SDLC, the Security Plan lists the actions needed to ensure that the system is developed in a reasonably secure environment and that it contains the sufficient and appropriate security features. It defines the security requirements and provides the step-by-step management plan to meet those requirements.

During the system's operation phase, the Security Plan becomes the action document for responding to new vulnerabilities and threats as well as serving as the primary basis for management reports. It must be updated at least annually, but may be updated more often prior to the system's operation phase.

Reference: Volume II, Chapter 1, Section C, *Tailoring Guidelines*, **Tailoring Security Deliverables**

Security Test Plan and Report

The Security Test Plan defines the planned activities, test data, and acceptance criteria for testing the security features of the delivered system. This plan is based, in part, on the user acceptance criteria initially identified in the User Requirements and agreed upon in the Functional Requirements.

The Security Test Report documents the result of the security testing. The Security Test Plan and Report becomes a supporting attachment to the Security Certification Statement.

Security Risk Assessment

The Security Risk Assessment documents the extent to which the application and the data it processes are or will be at risk. The risk assessment process includes defining and valuing the assets, defining the threats to those assets, determining the system's vulnerabilities, and recommending reasonable safeguards to bring the risks down to acceptable levels.

Security Design

The Security Design documents the philosophy of protection, the planned security architecture, and the mapping of each planned security feature to the security requirement(s) it is intended to satisfy.

Continued on next page

Document Descriptions, Continued

Security Features User's Guide

For all AIS's that have security features controlled by users (password selection, setting access control permissions, etc.), the Security Features User's Guide documents how those features are invoked and managed at the user level.

Note: This document does not cover the security feature suite intended for use by a security administrator or manager, which is covered in the Trusted Facility Manual.

Trusted Facility Manual

A Trusted Facility Manual (TFM) describes how to:

- Configure and install a specific secure system
- Operate the system in a secure manner
- Make effective use of the system privileges and protection mechanisms to control access to administrative functions and databases.

Reference: Further details are provided in NCSC-TG-016, *A Guide to Writing Trusted Facility Manuals*, October 1992.

Disaster Recovery/ Contingency Plan

This plan provides prescribed actions for dealing with anticipated future emergencies, failures, and disasters which could affect system operations.
It also includes a checklist of resource types and issues that should be considered when developing this type of plan.

Contingency Plan Test Report

The immediate response, alternate site processing, and reconstitution procedures in AIS contingency plans must be periodically tested. The results of those tests are captured in the Contingency Plan Test Report.

Security Certification Statement

This certification documents that the system passed all required security tests and therefore meets applicable security requirements.

System Accreditation Statement

Authorizes system operation under an acceptable level of risk.

Table 15-1. Security Deliverables - Create, Update, Revise, Baseline by Phase

		Development					
Deliverable	**Definition**	**Design**	**Program**	**Acceptance**	**Implementation**	**Operation**	**Evaluation**
Security Plan							
Development	C	U,B	R	R	R	R	-
Operation	-	-	-	-	-	C, U, B, R	-
Management Reports	C, B	R	R	R	R	R	-
Work Breakdown	C, B	R	R	R	R	R	-
Security Risk Assessment	C, B	R	R	R	R	R	-
Security Requirements							
Functional	C, B	R	R	-	-	-	-
Non-Functional	-	C, B	R	R	R	R	-
Security Design	-	C,B	R	-	-	-	-
Compliance with Vendor	-	-	C,B	R	R	R	-
System Interfaces	C, B	R	R	R	R	R	-
Rules of Behavior	C, B	R	R	R	R	R	-
Security Test Plan	C		B	R	-	-	-

C = Create U = Update (prior to baseline) R = Revise (after baselining if necessary) B = Baseline

Table 15-1. Security Deliverables - Create, Update, Revise, Baseline by Phase

Deliverable	Definitio n	Development			Implementation	Operation	Evaluation
		Design	Program	Acceptance			
Security Test Report	-	-	C	B	-	-	-
Configuration Plan	C, B	R	R	R	R	R	-
Trusted Facility Manual	C, B	R	R	R	R	R	-
User's Guide	-	C	B	R	R	R	-
Disaster Recovery Plan	C		B	R	R	R	-
Contingency Test Report	-	-	-	C	-	B, R	R
Contingency Plan	C	C	U	B	R	R	-
Training Plan	C	B	R	R	R	R	-
Application Audit	-	-	-	-	-	C, B, R	R
System Audit	-	-	-	-	-	C, B, R	R
Incident Response	-	-	-	-	-	C, B, R	-
Certification Report	-	-	-	C, B	R	R	R
Accreditation Report	-	-	-	C	B	R	R

C = Create U = Update (prior to baseline) R = Revise (after baselining if necessary) B = Baseline

Table 15-2. Prescribing Directives for Security Deliverables

Deliverable	Submit Every	Laws	OMB A-130	Treasury		Customs		Other
				P71-10	ISLC	SDLC	1400-05	
Plan						15/B		Also 6-G7-2e, 6-G8-2e
Development	Year	-	-	-	5-G4		-	
Operation	Varies	CSA	IIIA3a(2)	-	-		3.1.2	
Mgt. Reports	Year	CSA, PRA	IIIA3a(2)	-	5-G4		3.1.2	
Work Breakdown	Varies	-	-	-	1-M	-	-	-
Security Risk Assessment or Application Audit	3 Years	CSA, FMFIA	-	VI-7A1a	5-G5	7/B 15/D	3.2.2	Also A-123, A-127, etc
Requirements								
Functional	Varies	CSA,PA, etc	-	-	4-G1-8	14/C	Chapt. 4	Also 3.2.1
Non-Functional	Varies	PRA, etc.	-	-	-		Chapt. 4	Also 3.2.1
Design	Varies	PA, FOIA, etc.	-	VI-4B6d(4)	-	15/E	2.2(7)(c)	-
Compliance w/Vendor	Varies	-	-	VI-4B6e	-	10/C 17/C	-	-

CSA = Computer Security Act
PRA = Paperwork Reduction Act
PA = Privacy Act
FOIA = Freedom of Information Act

FMFIA = Federal Managers Financial Integrity Act

ISLC = Information System Life Cycle TD P 84-01
SDLC = Systems Development Life Cycle Handbook, CIS HB 5500-07

Table 15-2. Prescribing Directives for Security Deliverables

Deliverable	Submit Every	Laws	OMB A-130	Treasury		Customs		Other
				P71-10	ISLC	SDLC	1400-05	
System Interfaces	Varies	-	IIIA3a(2)(g)	-	-	10/C 17/C	2.2(7)(c)	-
Rules of Behavior	Year	-	IIIA3a(2)(a)	-	-	15/B	-	-
Test Plan	Varies	-	-	VI-4B6d(3)	5-G2-3a(5)	15/C	2.2(7)(c)	-
Test Report	Varies	-	-	VI-4B6d(3)	8-G-1d	15/C	2.2(7)(c)	-
Configuration Plan	Varies	-	-	VI-7A1b	-	15/B	-	-
Facility Manual	3 Years	-	-	VI-4B6d(2)	6-G3-2g	7/B 15/G	-	Also 6-G6-2c
User's Guide	Varies	-	-	VI4B6d(1)	6-G4-3d	15/F	-	-
Disaster Recovery Plan	Year	-	IIIA3a(2)(e)	-	-	7/B 15/H	3.1.3	-

CSA = Computer Security Act
PRA = Paperwork Reduction Act
PA = Privacy Act
FOIA = Freedom of Information Act

FMFIA = Federal Managers Financial Integrity Act

ISLC = Information System Life Cycle TD P 84-01
SDLC = Systems Development Life Cycle Handbook, CIS HB 5500-07

Table 15-2. Prescribing Directives for Security Deliverables

Deliverable	Submit Every	Laws	OMB A-130	Treasury		Customs		Other
				P71-10	ISLC	SDLC	1400-05	
Contingency Test Report	Year	-	IIIA3a(2)(e)	-	-	7/H 15/I	2.2(7)(c)	-
Contingency Plan	3 Years	-	IIIA3a(2)(e)	-	6-G9	7/B 15/H	3.1.3	Also 4-G2-5c
Training Plan	Varies	CSA	IIIA3a(2)(b)	VI-8A	6-G5-1e	7/B 15/F	3.6	-
Application Audit	3 Years	CSA, FMFIA	IIIA3b(3)	-	4-G2-8c	7/H	2.2(7)(c)	Also A-123, A-127
System Audit	Year	CSA, FMFIA	IIIA3a(3)	VI-4B6b(2)	6-G1-2e	7/H 15/J	2.2(7)(c)	A-123 A-127 10-G1-5

CSA = Computer Security Act
PRA = Paperwork Reduction Act
PA = Privacy Act
FOIA = Freedom of Information Act

FMFIA = Federal Managers Financial Integrity Act

ISLC = Information System Life Cycle TD P 84-01
SDLC = Systems Development Life Cycle Handbook, CIS HB 5500-07

Table 15-2. Prescribing Directives for Security Deliverables

Deliverable	Submit Every	Laws	OMB A-130	Treasury		Customs		Other
				P71-10	ISLC	SDLC	1400-05	
Incident Response	Varies	-	IIIA3a(2)(d)	VI-5B	-	-	Chapter 5	-
Certification Report	3 Years	CSA	IIIA3a(4)	VI-7A	9-G1	15/J	3.4.1	-
Accreditation Report	3 Years	CSA	IIIA2a(4)	VI-7A	9-G2	7/F 15/J	3.4.2	-

CSA = Computer Security Act
PRA = Paperwork Reduction Act
PA = Privacy Act
FOIA = Freedom of Information Act

FMFIA = Federal Managers Financial Integrity Act

ISLC = Information System Life Cycle TD P 84-01
SDLC = Systems Development Life Cycle Handbook, CIS HB 5500-07

Section B
Security Plan

Section Overview

The Security Plan is the first security deliverable that must be completed during the course of a project and is maintained throughout the project's life. It defines the security requirements of the system and the project at each phase of the project. The Security Plan also provides the step-by-step management and action plans to meet those requirements.

Responsibility

The Project Initiation Team is responsible for completing the initial version Security Plan. The initial version of the Security Plan must be provided to the Investment Review Board for preliminary project approval. The Security Plan must be updated after completion of each phase of the life cycle.

As the project moves through the life cycle, each revision/update to the Security Plan must be submitted to the AIS Security Team for their review and approval. The project may request assistance from the AIS Security Team.

References

The Security Plan is a major document and complete directions for writing one are beyond the scope of this SDLC. A basic annotated outline is provided below, and details can be found in such documents as:

- *Automated Information Systems Security Policy*, CIS HB 1400-05, Appendix D
- NIST's *User Guide for Developing and Evaluating Security Plans for Unclassified Federal Automated Information Systems*, July 1998

Also contact AISSD for additional supporting/explanatory material.

Continued on next page

Security Plan, Continued

In This Section

SECURITY PLAN

Project Name:		Project Number:	
Date Prepared:	Date Updated:	Date Presented:	Date Approved:

1.0 System Identification -- *This is the only information required in the initial phase of application development. The rest of the information is required for phases after approval to develop the application.*

1.1 Responsible Organization

1.2 System Name/Title/Acronym/MCP number

1.3 System Category

1.4 System Operational Status

1.5 General Description/Purpose

1.5.1 Business Process Description
1.5.2 Data Sensitivity Level
1.5.3 Proposed IT Architecture
1.5.4 Purpose of IT System

1.6 System Environment and Special Considerations

1.6.1 Description of basic data flows, network access, and architectural components, including graphic charts
1.6.2 Planned processes to construct databases/files (i.e., extraction)
1.6.3 Planned processes for user identification and authentication
1.6.4 Philosophy of Protection
1.6.5 Planned processes to audit security-relevant events
1.6.6 Planned use of cryptography
1.6.7 Planned use of electronic data interchange (EDI)
1.6.8 Planned output (e.g., report generation) processes
1.6.9 Planned interfaces with other applications and/or infrastructure
1.6.10 Planned compliance with Treasury's requirement for a C2 level of security
1.6.11 Planned processes to ensure that appropriate security features are built into the system

Continued on next page

SECURITY PLAN, Continued

1.0 System Identification (continued)

1.6.12 Planned security controls over the management and technical data generated and used by project participants
1.6.13 Work breakdown for security during development
1.6.14 Other

1.7 Information Contact(s)

1.7.1 Project Manager
1.7.2 Data Owner(s)
1.7.3 Business Sponsor(s)
1.7.4 Technical Leader(s)

1.8 Principal Approval Authorities

1.9 Other Information

1.10 References

1.10.1 Project Plan
1.10.2 USCS SDLC Handbook
1.10.3 USCS Architecture Guidelines
1.10.4 Primary Business Process Directives
1.10.5 Laws and Federal Directives Not Yet Implemented in USCS Directives
1.10.6 Prior Security Certifications (if any)

Continued on next page

SECURITY PLAN, Continued

2.0 Sensitivity of Information

This section identifies the sensitivity of the system contents. If this system/project is an application, use the following tables to describe the sensitivity information needed to identify the application requirements.

- **Table 1 - Data Sensitivity Categorization** identifies the data, the data classification, data category, and the data owners.
- **Table 2 - Data Protection Requirements** identifies the resulting security requirements of integrity, availability, and confidentiality. It also describes the data validation and encryption requirements.

If this system/project refers to a hardware platform or telecommunications network processing system, with applications covered in their own Security Plans, identify the application plans to be referenced rather than include the data tables here.

Table 1. Data Sensitivity Categorization (Examples are included)

Primary Data Category	Secondary Data Category	Data	Data Owner
Non-Sensitive Information	Unrestricted Public Information	Vacancy Announcements	Office of Personnel
Sensitive But Unclassified	Trade Secrets	Entry Summary Data Manifest Data	Office of Field Operations/ Office of Finance
Sensitive But Unclassified	Payroll Data	Payroll Data	Office of Finance

Continued on next page

SECURITY PLAN, Continued

The following Table identifies the various data classifications or categories in use at the Customs Service.

Primary Data Category	Secondary Data Category
Non-Sensitive Information	Unrestricted Public Information
Sensitive But Unclassified Information	Official Use Only Privacy Act Internal Administrative Procurement/Contract Limited Official Use Law Enforcement Financial - FMFIA Control Financial - Bank Secrecy Payroll Personnel Shippers Export Declaration Tax Trade Secrets Other Trade Information
Classified Information	Level of Classification

Table 2. Data Protection Requirements

The data protection requirements defined in Section 5.6 of the Functional Requirements document must be mapped to the specific security features in the design document to ensure that all requirements have been appropriately satisfied. This information should be available in the project's Requirements Traceability Matrix (RTM), if one exists, and can be referred to here rather than including this table.

Alternatively, pointers to the relevant sections of the Functional Requirements document and to the Security Design document may also meet the needs of this section and can be used instead of including the following table.

Reference: Volume II, Chapter 14, Section C, *Functional Requirements*, Section 5.6

Continued on next page

SECURITY PLAN, Continued

2.0 Sensitivity of Information (continued)

Table 2. Data Protection Requirements (continued)

Data	Integrity	Availability	Privacy/ Confidentiality

3.0 Rules of Behavior

As defined in OMB Circular A-130, these security-relevant rules should clearly delineate responsibilities of and expectations for all individuals with access to the system. These rules should address such issues as dial-in access, copyright protections, and individual accountability. The rules should also state the consequences of non-compliance and should form the basis for security awareness and training initiatives.

3.1 Generic *(This includes those rules identified in Automated Information Systems Security Policy, CIS HB 1400-05, Appendix B.)*

These are probably best addressed by referencing the applicable paragraphs in other documents.

3.2 System-Specific

Continued on next page

SECURITY PLAN, Continued

4.0 Security Risk Management and Accreditation

Reference the most recent security risk assessment of this system and provide an executive summary of its results. If none have been performed, state that fact and include the action plan for completing one.

Reference the most recent security accreditation of this system and describe any special constraints or limitations resulting from that accreditation. If none have been performed, state that fact and include the action plan for completing one.

5.0 System Security Measures

Security requirements are derived from laws, policies, and business needs, as tempered by anticipated risks. The previous sections identified the laws and regulations applicable to the data in this system and the risk management program. Control measures are used to mitigate the risks. Since most Customs data is *Sensitive But Unclassified*, there are certain minimum control measures Customs requires for all systems. In addition, the common environment provided by the Newington Data Center (NDC) may provide some of these controls.

Table 3. Security Control Measures

Control Measure	Description	Status/Schedule
Management	***Note:*** *This column may be satisfied by pointing to other locations/documents*	
Security Responsibility Assignment	*Example: See Project Plan*	
Rules of Behavior		
Risk Identification		
Risk Analysis		
Risk Prioritization		
Risk Management Planning		
Risk Resolution		
Risk Monitoring		

Continued on next page

SECURITY PLAN , Continued

5.0 System Security Measures (continued)

Table 3. Security Control Measures (continued)

Control Measure	Description	Status/Schedule
Personnel		
Personnel Screening		
Training (Security) - Developers/Maintenance - Customs Users - Trade Community - Other Agencies - Administrators - Operators		
User Agreements - Trade Community - Other Agency MOUs		
Acquisition/Implementation Controls		
Configuration Management		
Quality Assurance		
Requirement Specification		
Design Specification		
Security Test Plan		
Security Test Report		
Security Features User's Guide		
Security Features Administrator's Guide		
Trusted Facility Manual		
Certification Package & Accreditation Request		

Continued on next page

SECURITY PLAN, Continued

5.0 System Security Measures (continued)

Table 3. Security Control Measures (continued)

Control Measure	Description	Status/Schedule
Operations Controls		
Physical Protection		
Environmental Protection		
Production, I/O Controls		
Emergency Procedures		
Disaster Recovery Plan		
Application Contingency Plan		
Security Administration Controls		
User Addition & Deletion		
User Access Allowances and Monitoring		
User Activity Monitoring		
Audit & Variance Detection		
Data Management		
Computer Security Controls		
User Identification		
User Authentication		
Data Validation		
Access Controls		
Audit Trails Maintenance		
Audit Trail Analysis		
Real-time audit warnings		
System Architecture/Integrity		
Program Validation		
Trusted Path		
Encryption		

Continued on next page

SECURITY PLAN, Continued

6.0 User Roles and Access Requirements

Traditional access control required the maintenance of a list of authorized files for each user, including whether the user has CREATE, READ, UPDATE and/or DELETE permissions. These four permissions are often abbreviated CRUD. Today's systems typically involve far too many users for this to be a practical approach. Thus, the preferred approach is "role-based access control" (RBAC). In RBAC, access permissions are assigned to roles, rather than individuals. Each role is assigned the CRUD permissions. Individuals may assume concurrent roles and roles do not necessarily equate to job descriptions. These are security-relevant roles -- combinations of functional responsibility that equate to specific, pre-defined sets of access rights. There are fewer security roles than business roles, because many business roles require a common set of security access rights. Security roles must be defined for each application.

[Reserved for descriptions of user roles and access requirements. Include the tables providing the detailed assignments of data access to specific roles. Make sure these roles meet the segregation of duties requirement.]

7.0 Management Reports

Various reports of security planning activity are required and procedures to produce them must be documented in this paragraph. For example, the Computer Security Act of 1987 requires that a security report be sent to Congress every year for each major system, regardless of where it is in its life cycle. This annual report of security planning activity has been promulgated by various OMB bulletins (especially Bulletin 90-08) and is separate from the requirement to do security planning at the system level.

Continued on next page

SECURITY PLAN, Continued

8.0 Security Requirements

List all known security requirements or refer to appropriate locations in other documents.

8.1 Functional. The functional security requirements are those that provide for specific security features to be used by system users or security administrators.

8.2 Non-Functional. The non-functional security requirements provide no particular user or security administrator features, but are necessary because of architectural designs and/or broad mandates. Non-functional requirements are transparent to users and security administrators. They tend to be identified throughout the life cycle process, particularly during the design phase.

9.0 Action Plan

Provide a detailed plan for improving security, to include all dates, individuals, and actions.

10.0 Security Design

Provide the security design information here, or reference the documents (Security Design, System Design, etc.) that already provide that information. The outline provided for the Security Design document may be used as a guide for building subparagraphs under this item.

11.0 Additional Comments *[Reserved for any additional comments about the security of the subject system and any perceived need for guidance or standards.]*

Additional comments might include such subparagraph topics as:

- Plan for testing security-relevant features
- Configuration plan for both hardware and software
- Trusted facility (i.e., security administration) policies and procedures
- User’s guide to security features
- Contingency planning policies and procedures
- Security training plan

Note: As discussed in “Tailoring Security Deliverables” in Chapter 1, Section C, *Tailoring Guidelines*, each of these topics would normally be covered in a separate document if the project were for a large system, or may be included within other defined documents.

Section C
Security Test Plan and Report

Section Overview

There are two deliverables related to security testing:

- Security Test Plan
- Security Test Report

The Security Test Plan defines the planned activities, test data, and acceptance criteria for testing the security features of the delivered system. This plan is based, in part, on the user acceptance criteria initially identified in the User Requirements and agreed upon in the Functional Requirements.

The Security Test Report documents the results of the security testing and is often just an expansion of that document. The Security Test Plan and Report becomes a supporting attachment to the Security Certification Statement.

Responsibility

The System Development Team is responsible for producing the Security Test Plan and Report, based on their development efforts.

In addition, a group such as the System Acceptance Test (SAT) Team might be asked to provide an independent assessment of the development team's security testing. If so, that independent plan and report should be appended to the original plan and report.

The AIS Security Division must approve the Security Test Plan/results and may add additional tests to be performed.

In This Section

SECURITY TEST PLAN

Project Name:		Project Number:	
Date Prepared:	Date Updated:	Date Presented:	Date Approved:

1.0 The Plan

1.1 Software Description - Provide a chart and briefly describe the security features and functions of the software being tested as a frame of reference for the test descriptions.

1.2 Milestones - List the locations, milestones events, and dates for the testing.

1.3 Testing (Identify Location) - Identify the participating organizations and the location where the software will be tested.

1.3.1 Schedule - Show the detailed schedule of dates and events for the testing at this location. Such events may include familiarization, training, data, as well as the volume and frequency of the input.

1.3.2 Resource Requirements - State the resource requirements, including:

A. Equipment: Show the expected period of use, types, and quantities of the equipment needed.

B. Software: List other software that will be needed to support the testing that is not part of the software to be tested.

C. Personnel: List the numbers and skill types of personnel that are expected to be available during the test from both the user and development groups. Include any special requirements such as multi-shift operation or key personnel.

1.3.3 Testing Materials - List the materials needed for the test, such as:

A. Documentation
B. Software to be tested and its medium
C. Test inputs and sample outputs
D. Test control software and worksheets

Continued on next page

SECURITY TEST PLAN, Continued

1.0 The Plan (continued)

1.3.4 Test Training - Describe or reference the plan for providing training in the use of the security software being tested. Specify the types of training, personnel to be trained, and the training staff.

1.4 Testing (Identify Location) - Describe the plan for the second and subsequent locations where the software will be tested in a manner similar to paragraph 1.3.

2.0 Specifications and Evaluation

2.1 Specifications

2.1.1 Software Functions - List the detailed software security and privacy features to be exercised during the overall test.

2.1.2 Test/Function Relationships - List the tests to be performed on the software and relate them to the features in paragraph 2.1.1.

2.1.3 Test Progression - Describe the manner in which progression is made from one test to another so that the entire test cycle is completed.

2.2 Methods and Constraints

2.2.1 Methodology - Describe the general method or strategy of the testing.

2.2.2 Conditions - Specify the type of input to be used, such as live or test data, as well as the volume and frequency of the input.

2.2.3 Extent - Indicate the extent of the testing, such as total or partial. Include any rationale for partial testing.

2.2.4 Data Recording - Discuss the method to be used for recording the test results and other information about the testing.

2.2.5 Constraints - Indicate anticipated limitations on the test due to test conditions, such as interfaces, equipment, personnel, databases.

Continued on next page

SECURITY TEST PLAN, Continued

2.0 Specifications and Evaluation (continued)

2.3 Evaluation

2.3.1 Criteria - Describe the rules to be used to evaluate test results, such as range of data values used, combinations of input types used, maximum number of allowable interrupts or halts.

2.3.2 Data Reduction - Describe the techniques to be used for manipulating the test data into a form suitable for evaluation, such as manual or automated methods, to allow comparison of the results that should be produced to those that are produced.

3.0 Test Descriptions

3.1 Test 1 (Identify) - Describe the test to be performed.

3.1.1 Control - Describe the test control, such as manual, semi-automatic, or automatic insertion of inputs, sequencing of operations, and recording of results.

3.1.2 Inputs - Describe the input data and input commands to be used during the test.

3.1.3 Outputs - Describe the output data expected as a result of the test and any intermediate messages that may be produced.

3.1.4 Procedures - Specify the step-by-step procedures to accomplish the test. Include test setup, initialization, steps, and termination.

3.x Test x (Identify) - Describe the second and subsequent tests in a manner similar to that used in paragraph 3.1.

SECURITY TEST REPORT

Project Name:		Project Number:	
Date Prepared:	Date Updated:	Date Presented:	Date Approved:

1.0 Executive Summary - Summarize the overall conclusions of the testing team, and list the major Conclusions and Recommendations contained in the report.

1.1 Introduction - Provide a background on the program for the benefit of agency officials and others who are not familiar with the authorities under which these tests are conducted.

1.2 Conclusions and Recommendations - Describe each conclusion and recommendation as summary statements or bullets only.

2.0 Purpose of the Tests - Objective(s) - State the purpose and objective(s) defined for the tests.

3.0 Methodology - Describe how the testing was conducted, measurement criteria, etc.

4.0 Major Findings and Conclusions - Each summary statement listed in the Executive Summary should serve as a heading in this section of the report. Each issue should reflect factual evidence and present an evaluation of the positive/negative impact on areas affected by the tests.

5.0 Major Recommendations - State the overall impressions (conclusions) of the testing team. Then explain in more detail the recommendations listed in the Executive Summary.

6.0 Initiatives and Actions - Explain how the recommendations are being addressed. What initiatives or actions are planned and when they are scheduled.

7.0 Benefits of the Review - Describe the benefits (i.e., savings, performance, resources) uncovered as a result of the tests.

8.0 Appendices - Include acronyms used in the report and supporting documentation as deemed necessary.

Section D
Security Risk Assessment

Introduction

Security risk is the potential for an IT system, particularly the electronic data it processes and stores, to suffer from any unauthorized modification, destruction, disclosure, or delay in availability. This focus on IT resources distinguishes security risks from project risks (i.e., budget overruns and schedule delays) and system risks (i.e., ineffective operation and inefficient operation), although in practice there may be some overlaps in these three types of risk.

Security risk assessments vary from informal, qualitative reviews of small applications to formal, quantitative assessments of major computer centers. Regardless of scope, they all measure and assess the vulnerabilities of and threats to electronic data and the people, systems and installations involved in storing and processing that data.

Security Risk Assessment Process Steps

The essential six steps in the security risk assessment process are:

(1) Determine the type of assessment (whether it's a system or an application, which life cycle phase it's in, etc.),

(2) Define and characterize the system (data, hardware, software, etc.),

(3) Review the security requirements (according to applicable security directives and appropriate business process needs),

(4) Identify threats to and vulnerabilities of the AIS resources,

(5) Calculate risks and propose new or revised controls (if appropriate), and

(6) Obtain management acceptance of residual security risks.

Reference: Also see the suggested activities in Chapter 5, *Risk Management Processes*, for generic project risk identification and prioritization techniques.

Continued on next page

Security Risk Assessment, Continued

Life Cycle Considerations

The initial security risk assessment occurs during the Definition Phase and will be somewhat skeletal. However, the assessment process is ongoing and becomes the basis for many security requirements.

A final Security Risk Assessment is a mandatory supporting document for the Security Accreditation that precedes implementation. Operational systems must undergo a security risk assessment whenever:

- The system undergoes a significant modification,
- The system's environment changes significantly, or
- Five years have elapsed since the last security risk assessment.

Responsibility

For systems in the pre-operations phase, the System Development Team is responsible for performing the security risk assessment and producing the Security Risk Assessment report.

Once operational, this becomes the responsibility of the system's Business Sponsor (e.g., owner).

References

For further guidance on conducting and documenting a Security Risk Assessment see:

- Department of the Treasury's *Risk Assessment Guideline*, TD P 85-03 Volumes I and II, June 1990

- *Automated Information Systems Security Policy*, CIS HB 1400-05, June 1996

Note: Treasury's *Risk Assessment Guideline* provides a set of 22 worksheets and 28 resource tables that provide a self-documenting risk assessment process. When used, the Treasury process obviates the need for the report format template outlined below.

In This Section

SECURITY RISK ASSESSMENT

Project Name:		Project Number:	
Date Prepared:	Date Updated:	Date Presented:	Date Approved:

1.0 Executive Summary

1.0 Executive Summary - Summarize the overall conclusions of the review team, and list the major conclusions and recommendations.

1.1 Introduction - Provide a brief background on the project for the benefit of agency officials and others who are not familiar with it.

1.2 Conclusions and Recommendations - List each conclusion and recommendation as a bullet list or brief statements.

2.0 Purpose of the Risk Assessment - Objective(s) - State the purpose and objective(s) defined for the risk assessment.

3.0 Methodology - Describe how the risk assessment was conducted, measurement criteria used, etc.

4.0 Prior Results - Describe the results of prior security monitoring and reviews.

4.1 Development Testing
4.2 Operations Testing
4.3 Security Monitoring/Reviews
4.4 Internal Audits
4.5 External (i.e., Independent) Audits
4.6 Security Risk Assessments

5.0 Vendor Recommendations - Explain the extent to which the system is in compliance with security-relevant vendor recommendations for all generic (i.e., COTS) products.

Continued on next page

SECURITY RISK ASSESSMENT, Continued

6.0 Findings and Conclusions - For each potential threat assessed, there should be factual evidence and an evaluation the impact on the system.

7.0 Recommendations - Explain in more detail the recommendations listed in the Executive Summary.

8.0 Initiatives and Actions - Explain how the recommendations are being or will be addressed. What initiatives or actions are planned and when are they scheduled?

Appendices - Include acronyms used in the report and supporting documentation deemed necessary.

Section E
Security Design

Introduction

The information identified in these guidelines must be developed by all projects during the design phase and tracked during development.

Based on the size of a project, this information can be included within the System Design document **or** described in a separate document as defined here. The outline provided below can also be used to identify the information to be included in the System Design and/or the Security Plan.

The System Design document contains a technical description of data structures, planned system functionality, and an overview of the planned security features. However, a separate Security Design document is normally required for large systems. It provides a much more detailed description of the target security architecture, features, and component interdependence.

Responsibility

For systems in the pre-operations phase, the System Development Team is responsible for producing and maintaining the Security Design, in consultation with the AIS Security Division (AISSD).

Once the system is operational, this information and documentation becomes the responsibility of the Business Sponsor (i.e., system's owner).

References

For further guidance on producing a Security Design, see:

- National Computer Security Center's *A Guide to Understanding Design Documentation in Trusted Systems*, NCSC-TG-007, October 2, 1988
- Department of the Treasury *Security Manual*, TD P 71-10, October 1992
- *Automated Information Systems Security Policy*, CIS HB 1400-05, June 1996
- Customs' *Enterprise IT Architecture Strategy*, July/August 1997

In This Section

SECURITY DESIGN

Project Name:		Project Number:	
Date Prepared:	Date Updated:	Date Presented:	Date Approved:

1.0 Security Overview - Provide an overview of the security system to be developed.

1.1 System Purpose - Describe the purposes for this system in terms of Customs business processes and the overall IT context. Reference any other documents (System Design, Project Plan, etc.) that describe these system purposes in more depth.

1.2 Definitions - Define key terms.

1.3 Boundaries - Describe the scope of security concerns and issues in terms of the system's planned and/or actual physical boundaries, electronic connectivity, interfaces with other systems, dependence on IT infrastructure, etc.

1.4 Security Purpose - Describe the security purposes for this system in terms of availability, integrity, confidentiality, and trust (including nonrepudiation). State whether the system must exceed the Customs standard C2 level security and whether records are governed by the Privacy Act or Trade Secrets Act.

1.5 Security Requirements - Summarize the functional and non-functional security requirements for this system. Reference any other documents that describe these requirements in greater detail.

2.0 Philosophy - Describe the overall philosophy of protection in terms of how the broad security features and techniques are intended to appropriately preserve the defined needs for availability, integrity, confidentiality, and trust. This philosophy represents the unifying grand security design chosen to meet the defined requirements.

3.0 Scope - Describe the intended scope of security within this system, including the extent to which standard Customs infrastructure will be expected to provide security services.

Continued on next page

SECURITY DESIGN, Continued

4.0 Assumptions

- List the primary assumptions that underlie the planned and/or actual security architecture.

5.0 Trusted Computing Base

- The trusted computing base (TCB) is the totality of protection mechanisms (i.e., one or more hardware/software components) within a computer system that are responsible for internally enforcing the security rules established to manage, protect, and distribute sensitive information. Describe the TCB for this system.

5.1 Overview - Describe the main security components of the TCB and how they are intended to interact.

5.2 Security Services - Describe each of the planned security features and describe who will be responsible for invoking each.

5.3 Self-Protection - Describe how the TCB will protect itself, during operation, from unauthorized or unplanned modifications and delays in availability. If there are portions of the TCB that must be protected from unauthorized disclosure, describe those protection mechanisms as well. If there are no confidentiality or privacy requirements for the TCB itself, state that fact.

5.4 Level of Trust - Describe the required level of assurance that the TCB does, indeed, do what it is intended to do, and no more. Outline the processes, procedures, and products planned to provide that level of assurance.

6.0 Alternative Security Designs

- Describe each alternative security design considered. If no alternatives were considered, state that fact.

7.0 Mapping of Features to Requirements

- Describe how the planned/actual architecture will satisfy the defined security requirements. Include a mapping of each planned/actual security feature to the security requirement(s) it is intended to satisfy.

Note: If a Requirements Traceability Matrix (RTM) is used on the project, this requirements and design feature mapping cross-reference section can be satisfied by referring to the appropriate section(s) of the RTM.

Section F
Security Features User's Guide

Introduction

The Security Features User's Guide (SFUG) describes how system users (excluding system security administrators/managers) should use the planned security features (e.g., password selection, setting access control permissions, etc.).

The SFUG documents how those features are invoked and managed at the user level, but does not cover the security feature suite intended for use by a security administrator or manager, which is covered in the Trusted Facility Manual.

Responsibility

For systems in the pre-operations phase, the Training Branch, in conjunction with the System Development Team and AISSD, is responsible for producing and maintaining the information documented in the SFUG.

Note: Based on the size of the project and/or the complexity of the security features included, this information can be included within the system's User Manual, or described in a separate document as defined here.

Once the system is operational, it becomes the responsibility of the Business Sponsor (i.e., system's owner) to ensure that this document is maintained as changes occur.

References

For further guidance on producing a SFUG, see:

- National Computer Security Center's *A Guide to Writing the Security Features User's Guide (SFUG) for Trusted Systems*, NCSC-TG-026, September 1991
- Department of the Treasury *Security Manual*, TD P 71-10, October 1992
- *Automated Information Systems Security Policy*, CIS HB 1400-05, June 1996

In This Section

Topic	See Page
Security Features User's Guide Template/Guidelines	II-15-38

SECURITY FEATURES USER'S GUIDE

Project Name:		Project Number:	
Date Prepared:	Date Updated:	Date Presented:	Date Approved:

1.0 Introduction - Provide an overview of the SFUG.

1.1 SFUG Purpose - Describe the purpose of this document.

1.2 Target Audience - Define the intended categories of people who are expected to read/use the SFUG.

1.3 Outline - Describe the format of the SFUG for this system.

1.4 References - List other documents that readers may wish to review for more information.

2.0 Overview - Describe the overall system's security in non-technical terms.

2.1 Philosophy of Protection

2.1.1 Environment - Describe the general environment for which the system is designed.

2.1.2 Approach - Describe the overall approach taken to provide reasonable protections against the unauthorized or unplanned modification, destruction, disclosure, and delays in availability of the user's electronic information.

2.1.3 Motivation - Describe why the protection approach was chosen and how the environment motivated that decision.

2.2 Definitions - Define key term and abbreviations

2.3 System Security Administrator/Officer - Describe the roles and responsibilities of the security officer, as they relate to system users.

2.4 User Responsibilities - Describe the system user's security responsibilities. These "rules of behavior" should clearly delineate the responsibilities of and expectations for all individuals with access to the system.

Continued on next page

SECURITY FEATURES USER'S GUIDE, Continued

3.0 User Commands - Describe how users are expected to invoke and use their security features/services.

3.1 User Identification and Authentication (I&A)

3.1.1 Identification - Describe how users are expected to log onto the system and identify themselves.

3.1.2 Authentication - Describe the user procedures for authenticating their identification using passwords, smartcards, etc. Provide user level guidance for selecting proper passwords, if applicable.

3.1.3 Changes - Describe the policies and procedures for users to change their group membership and other hierarchical associations relative to their I&A.

3.1.4 Session Termination - Provide the user procedures for logging off the system.

3.1.5 Errors - Describe the anticipated I&A user errors and their causes.

3.2 Discretionary Access Control (DAC)

3.2.1 Settings - Describe how users are expected to set/unset access permissions to named objects. (These are defined as "discretionary" because they are set at a user's discretion.)

3.2.2 Defaults - Describe the default DAC permissions. (These are the assumed or automatic settings for discretionary access, but do not include the mandatory access control, or MAC, settings managed by security administrators/officers.)

3.2.3 User Groups - Describe the policies and procedures for users to establish user group memberships and other hierarchical associations relative to their I&A, as applicable.

3.2.4 Errors - Describe the anticipated DAC errors and their causes.

Continued on next page

SECURITY FEATURES USER'S GUIDE, Continued

3.0 User Commands (continued)

3.3 Object Manipulation

3.3.1 Objects - Describe how users are expected to create data files, executable processes, and other objects. Also, describe how users may reuse and/or delete these objects.

3.3.2 Imports - Describe the policies and procedures for users to import electronic objects from other systems into this one.

3.3.3 Exports - Describe the policies and procedures for users to export electronic objects from this system into other systems.

3.3.4 Properties - Provide the user procedures for determining the security relevant properties of objects.

3.3.5 Errors - Describe the anticipated object manipulation errors and their causes.

3.4 Event Logging/Reporting - Describe the user level policies and procedures for documenting and/or reporting security-relevant events.

3.5 Other Security-Related Commands for Users

Section G
Trusted Facility Manual

Introduction

The Trusted Facility Manual (TFM) is a manual for security managers, rather than users. It defines the security concepts, procedures, and operations needed for day-to-day security administration of the system.

Responsibility

The System Development Team is responsible for writing the TFM, because they best understand the security feature set and how it was designed to be used. Assistance and examples can be obtained from AISSD.

Once the system is operational, the Business Sponsor (i.e., system owner) is responsible for maintaining the TFM.

References

For further guidance on the preparation of this manual, refer to *A Guide to Understanding Trusted Facility Management*, NCSC-TG-015, and *A Guide for Writing Trusted Facility Manuals*, NCSC-TG-016. Contact AISSD for copies.

In This Section

TRUSTED FACILITY MANUAL

Project Name:		Project Number:	
Date Prepared:	Date Updated:	Date Presented:	Date Approved:

1.0 Introduction

1.1 Purpose

1.2 Scope

1.3 Contents

1.4 References

2.0 System Security Overview

2.1 Overview of the Facility/Site

2.2 Application Level Security

2.3 Protection Measures Only Available to Security Administrators

3.0 Security Administrator Commands, Calls, and Functions

3.1 User Identification and Authentication (I&A)

3.1.1 Adding Users and Groups
3.1.2 Deleting Users and Groups
3.1.3 Assigning Initial Passwords
3.1.4 Changing Passwords

3.2 Discretionary Access Control (DAC)

3.3 Mandatory Access Control (MAC)

Continued on next page

TRUSTED FACILITY MANUAL, Continued

3.0 Security Administrator Commands, Calls, and Functions (continued)

3.4 Security Monitoring and Auditing

3.4.1 Setting Features/Flags
3.4.2 Building Security/Audit Databases
3.4.3 Analyzing Security/Audit Databases
3.4.4 Responses to Security Incidents

3.5 Security of the Trusted Computing Base (TCB)

3.5.1 Generation of Code
3.5.2 Configuration Management (CM)
3.5.3 Installation Procedures
3.5.4 Maintenance Procedures
3.5.5 Distribution Procedures

3.6 Other Commands, Calls, and Functions

4.0 Warnings of Vulnerabilities

4.1 User I&A

4.2 DAC

4.3 MAC

4.4 Security Monitoring and Auditing

4.5 Security of the TCB

4.6 Other Functions

Section H
Disaster Recovery/Contingency Plan

Overview

A Contingency Plan is an action plan for ensuring IT processing continuity despite catastrophic events. Contingency Plans cover three types of actions:

- Emergency procedures for initially responding to disruptions at primary locations,
- Backup procedures for conducting operations at alternate locations, when necessary, and
- Recovery procedures for restoring normal operations back at the primary locations.

A Contingency Plan is required to be developed for each application/system and approved before system implementation.

Responsibility

The System Development Team is responsible for drafting the initial Contingency Plan, because they best understand the system and how it was intended to be used.

AIS Security, User Support Services, and the Systems Operations Division may all assist in its development. The Business Sponsor approves the system's Contingency Plan during the Acceptance Phase.

Once the system is operational, the Business Sponsor (i.e., system owner) is responsible for maintaining the Contingency Plan, in coordination with those organizations that maintain the OIT Disaster Recovery Plan, the Customs Business Continuity Plan, etc.

Continued on next page

Disaster Recovery/Contingency Plan, Continued

References

For further guidance on producing a Contingency Plan, see:

- Federal Information Processing Standard Publication (FIPS PUB) 87, *Guidelines for ADP Contingency Planning*, March 1981
- Department of the Treasury *Security Manual*, TD P 71-10, October 1992
- *Automated Information Systems Security Policy*, CIS HB 1400-05, June 1996

In This Section

DISASTER RECOVERY/CONTINGENCY PLAN

Project Name:		Project Number:	
Date Prepared:	Date Updated:	Date Presented:	Date Approved:

A contingency plan is an action plan for ensuring processing continuity for all mission-critical systems.

Application/system contingency plans are **required** to be developed and must contain the following:

1.0 Description - Provide a description of the application/system, including each function it performs. This information can be extracted from the final set of User and Functional Requirements.

2.0 Users - List the user(s) dependent upon the application/system, including their organization and telephone numbers.

Example: Airport Passenger Inspection (API) System

User Name	Telephone Number(s)	Impact
Airport Passenger Inspection System Business Sponsor/ Process Owner	Work Number Home Number Beeper Number	• Customs personnel at international airports would be unable to process international travelers or perform API.
INS Contact	Work Number Home Number Beeper Number	• At many airports, INS uses this system to screen incoming passengers before they reach the Customs area.

Suggestion: To avoid the need to update this document each time specific users change, it may be possible to create the user name/phone number list in this document as a linked table from a database of users.

Continued on next page

DISASTER RECOVERY/CONTINGENCY PLAN, Continued

3.0 Resources - Identify the resources required to process the application/system (e.g., hardware, software, communications, and personnel). Issues and items to be considered include (but are not necessarily limited to):

Resource Type	Includes
People	• Employees and Contractors • Permanent and Temporary • Age and Gender • Host and Remote • Managers and Technicians
Data	• Electronic and Manual • Current and Historical • Host and Remote
Software	• Application Infrastructure • Source and Object Code • Configurations and Modifications • Current and Planned
Hardware	• Computers and Communications • Primary and Back-up • Purchased and Leased • Current and Planned • Client/Server
Communications	• Voice and Digital • Local and Long Distance • Primary and Back-up • Purchased and Leased • Current and Planned • Telephones and Ports • Protocols and Addresses • Routers and Firewalls • Cables and Towers • Immediate and Long-Term

Continued on next page

DISASTER RECOVERY/CONTINGENCY PLAN, Continued

3.0 Resources (continued)

Resource Type	Includes
Supplies	• Food and Water • Office Supplies • Forms and Media • Transport and Storage • Immediate and Long Term
Transportation	• Car and Bus • Plane and Train • Boat and Truck • Primary and Back-up • Purchased or Lease • Current and Planned
Documentation	• Policies and Procedures • Contacts and Contracts • Host and Remote • Hardware and Software • IT Process and Business Process • Installation and operation • Primary and Back-up • On-line and Hard Copy
Facilities	• Showers and Toilets • Power and Water • Heat and Air Conditioning • Office and Operations • Host and Remote • Customer and Service Provider

4.0 Sensitivities - Identify the sensitivity designation for the application/system and the security requirements needed during and after processing.

Continued on next page

DISASTER RECOVERY/CONTINGENCY PLAN, Continued

5.0 Actions - Describe the actions that must be taken to continue processing during specific emergency situations. Situations and actions could be tabled for quick reference.

Example:

Situation	Action(s)	Verification
Newington Data Center loses electrical power	The building monitoring system should change over to battery power within x.x seconds.	Check to see that change over has been done.
	Notify Power Company at (703) XXX-YYYY	Be sure to get the name of person notified and service order number.
	Arrange for back-up generator from XYZ Supplier at (703)XXX-YYYY.	Be sure to get the name of person notified and service order number.

6.0 Instructions - Provide any additional details or instructions necessary to continue application/system processing during and after an emergency.

Signed:____ Date:_____________
Business Sponsor

Signed:____ Date:_____________
Project Manager

Section I
Contingency Plan Test Report

Introduction

Contingency Plans must be tested periodically and the results of those tests must be captured in a Test Report.

Responsibility

Typically, the Contingency Plan is not completely tested until the system is fully operational. Thus, the Business Sponsor (i.e., system owner) is responsible for testing the Contingency Plan and producing the Contingency Plan Test Report.

The System Development Team and AISSD may provide assistance in the test and report development, as requested.

In This Section

CONTINGENCY PLAN TEST REPORT

Project Name:		Project Number:	
Date Prepared:	Date Updated:	Date Presented:	Date Approved:

1.0 Executive Summary - Summarize the overall conclusions of the testing team, and list the major Conclusions and Recommendations contained in the report.

1.1 Introduction - Provide a background on the program for the benefit of agency officials and others who are not familiar with the authorities under which these tests are conducted.

1.2 Conclusions and Recommendations - Describe each conclusion and recommendation as summary statements or bullets only.

2.0 Purpose of the Tests - Objective(s) - State the purpose and objective(s) defined for the tests.

3.0 Methodology - Describe how the testing was conducted, measurement criteria, etc.

4.0 Major Findings and Conclusions - Each summary statement listed in the Executive Summary should serve as a heading in this section of the report. Each issue should reflect factual evidence and present an evaluation of the positive/negative impact on areas affected by the tests.

5.0 Major Recommendations - State the overall impressions (conclusions) of the testing team. Then explain in more detail the recommendations listed in the Executive Summary.

6.0 Initiatives and Actions - Explain how the recommendations are being addressed. Include what initiatives or actions are planned and when they are scheduled.

7.0 Benefits of the Review - Describe the benefits (i.e., savings, performance, resources) uncovered as a result of the tests.

8.0 Appendices - Include acronyms used in the report and supporting documentation as deemed necessary.

Section J
Certification and Accreditation Statements

Section Overview

Since 1978, the federal government (through the Office of Management and Budget [OMB]) has required a Security Certification Statement for each ADP system. This Security Certification must proceed the Security Accreditation, in which senior management formally accepts all residual security risks for the system.

The Security Accreditation must be signed prior to the system becoming operational. ADP systems must then be re-accredited whenever significant changes occur, and at least every three years.

Definitions

Security Certification: A Security Certification is a formal statement by management about the extent to which an ADP system:

- Meets its defined security requirements,
- Is in compliance with all applicable policies and directives, and
- Has reasonable security controls.

The Security Certification is based on comprehensive tests and evaluations of the technical (i.e., hardware and software) features of the system as well as reviews of the related administrative, personnel, and physical safeguards anticipated for the system's environment.

Security Accreditation: The Security Accreditation Statement is senior management's formal acceptance of all residual security risks. In effect, it is senior management's "buy off" on the Security Certification Statement, which would be attached, including all of its attachments.

Security Certification Responsibility

Definition: The Designated Security Officer (DSO) for the system is responsible for:

- Overseeing all security certification activities
- Preparing the Security Certification Statement
- The security of the application in the operational environment

The Business Sponsor and the System Development Team will together ensure that all required attachments are available for the Certification Package.

Continued on next page

Certification and Accreditation Statements, Continued

Security Certification Responsibility (continued)

The Information Systems Security Officer (ISSO) is responsible for reviewing the Security Certification Package and certifying that the application has been tested and found to meet all applicable Federal policies, regulations, and standards for securing information systems and the data that will be processed by them.

Note: The Customs ISSO is designated as the Director, AIS Security Division.

Security Accreditation Responsibility

The Customs Business Sponsors/Process Owners (POs) are responsible for the security accreditations for all business processes for which they have responsibility.

In addition, the Assistant Commissioner, OIT, serves as the Principal Accrediting Authority (PAA).

Thus, the POs and the PAA share the security accrediting responsibility.

In This Section

SECURITY CERTIFICATION STATEMENT

FOR THE *[Insert System Name]* **SYSTEM**

NOTE: *Contact AIS Security Division for preparation instructions and assistance.*

I have carefully considered the security and integrity requirements and vulnerabilities of the system indicated above. Having complied with the requirements for documenting its sensitivity and value, assessing risks and vulnerabilities, identifying safeguards, and preparing a Contingency Plan, I recommend granting this AIS (check one).

□ Accreditation with Approval to Operate.

□ Provisional Accreditation with Approval to Operate pending implementation of safeguards identified on the attached schedule. Period of accreditation is **6 months.**

□ Provisional Accreditation with Approval to Operate pending submission of Sensitive Application Certification Statements.

□ Accreditation with Approval to Operate under the condition that the following additional safeguards be planned or restrictions enforced:

____

____

□ Other than Approval to Operate: (explain)

____

____

Signed:____ Date:______________
Designated Security Officer

Signed:____ Date:______________
Information Systems Security Officer

Attachments

1. Security Plan
2. Security Test Plan and Report
3. Updated Security Risk Assessment
4. Security Design
5. Security Features User's Guide
6. Trusted Facility Manual
7. Contingency Plan
8. Security Certification Summary and Recommendation
9. Formal Requests for Policy Waivers

SECURITY ACCREDITATION STATEMENT

FOR THE *[Insert System Name]* **SYSTEM**

NOTE: *Contact the AIS Security Division for the Accreditation Package and guidance in its preparation.*

We have examined the materials submitted to support security accreditation of :

System Name: ____
Located at: ____
____

Based on this examination, we authorize this system to process information rated:

□ Classified
□ Sensitive But Unclassified
□ Non Sensitive

Subject to the following conditions:

____
____
____
____
____

Signed:____ Date:_____________
Assistant Commissioner
Office of Information and Technology

Signed:____ Date:_____________
Assistant Commissioner
(Supervisor of Business Sponsor/Process Owner)

Attached:

Security Certification Statement and its attachments

This page intentionally blank